Jennifer Lynch (SBN 240701)
jlynch@eff.org
Hanni M. Fakhoury (SBN 252629)
hanni@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for *Amicus Curiae*
ELECTRONIC FRONTIER FOUNDATION

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE TELEPHONE INFORMATION NEEDED FOR A CRIMINAL INVESTIGATION

Case No.: 3:14-xr-90532-NC-1

BRIEF *AMICUS CURIAE* OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF A WARRANT REQUIREMENT FOR HISTORICAL CELL SITE INFORMATION

Courtroom A, 15th Floor
Hon. Nathanael Cousins

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

State Cases

Federal Statutes

State Statutes

Federal Constitutional Provisions

State Constitutional Provisions

State Legislative Materials

Other Authorities

INTRODUCTION

In the more than 35 years since the Supreme Court decided *Smith v. Maryland*, 442 U.S. 735 (1979), the capacity for technology to reveal unexpectedly detailed information about our lives has increased exponentially year after year. Where, in *Smith*, the government was able to record the numbers dialed and received on one phone at one location for three days, now the government can obtain not just those numbers but also information about all the locations where the phone's owner traveled during the entire time the phone was capable of receiving or making a call. This technology was "nearly inconceivable just a few decades ago." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). As the Supreme Court recognized in *Kyllo v. United States*, given these advances in technology, courts must increasingly face the question of "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." 533 U.S. 27, 34 (2001).

Courts and legislatures across the country are responding by pushing beyond the case law of 35 years ago and enacting greater privacy protections for the data we store on our technical devices, in the "cloud," and with third parties. As more Americans have a subjective expectation of privacy in their data, these expectations necessarily become ones that "society is prepared to recognize [are] 'reasonable,'" and thus protected by the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). This Court should follow this clear trend and require the government to use a probable cause search warrant to obtain historical cell site records.

ARGUMENT

I. AMERICANS HAVE AN EXPECTATION OF PRIVACY IN THE LOCATION INFORMATION GENERATED BY THEIR CELL PHONES.

Owning a cell phone is not a luxury; today more than 90%[1] of all American adults have a cell phone, and landline phones are becoming increasingly obsolete.[2] Through historical cell site

[1] Pew Research Center, "Cell Phone Ownership Hits 91% of Adults," (June 6, 2013) http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

[2] *See* National Journal, "Americans Continue to Drop Their Landline Phones," (December 18, 2013) http://www.nationaljournal.com/hotline-on-call/americans-continue-to-drop-their-landline-phones-20131218 (citing CDC statistics finding 38% of U.S. adults live in household with no landline phone).

information—the records of which cell phone towers a cell phone customer connects to and when—these cell phones generate a staggering amount of data about where the cell phone's owner has travelled throughout her daily life—data that is available to law enforcement.

Society is increasingly recognizing that location data like this deserves "the most scrupulous protection from government invasion." *Oliver v. United States*, 466 U.S. 170, 178 (1984) (citing *Payton v. New York*, 445 U.S. 573 (1980)). A court reviewing the appropriate Fourth Amendment limits to be placed on searches of and by new technologies must necessarily look to "societal understandings" of what should be considered private to determine what privacy expectations are reasonable. *Oliver*, 466 U.S. at 178; *see also Rakas v. Illinois*, 439 U.S. 128, 143 n. 12 (1978) (Fourth Amendment "expectation of privacy" must "have a source outside of the Fourth Amendment" by referencing "understandings that are recognized and permitted by society."). That ensures the Fourth Amendment remains a manifestation of society's belief that it chooses "to dwell in reasonable security and freedom from surveillance." *Johnson v. United States*, 333 U.S. 10, 14 (1948).

This societal recognition of privacy in historical cell site information and other telephone records is reflected in recent federal and state cases and statutes deeming this data to be private. While, the Fourth Amendment is not dependent on any specific state's laws, *see California v. Greenwood*, 486 U.S. 35, 43 (1988), federal courts have not hesitated to look to state law to determine whether an expectation of privacy is reasonable. *See United States v. Maynard*, 615 F.3d 544, 564 (D.C. Cir. 2010) ("state laws are indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable"); *see also United States v. Velasquez*, No. CR-08-0730-WHA, 2010 WL 4286276, *5 (N.D. Cal. Oct. 22, 2010) (unpublished) ("the recognition of a privacy right by numerous states may provide insight into broad societal expectations of privacy").

Similarly, while the Fourth Amendment is not "a redundant guarantee of whatever limits on search and seizure legislatures might have enacted," *Virginia v. Moore*, 553 U.S. 164, 168 (2008), the existence of both federal and state statutory protection for certain kinds of information helps

inform whether society has determined that a particular expectation of privacy is reasonable. *See, e.g., United States v. Nerber*, 222 F.3d 597, 604-05 (9th Cir. 2000) (federal wiretap statute is "strong evidence" that society would find warrantless video surveillance unreasonable); *Doe v. Broderick*, 225 F.3d 440, 450 (4th Cir. 2000) (federal statutory protection "is relevant to the determination of whether there is a 'societal understanding'" of a legitimate expectation of privacy in medical records); *Trujillo v. City of Ontario*, 428 F. Supp. 2d 1094, 1106 (C.D. Cal. 2006) (California statutes governing video surveillance in locker rooms and restrooms represent "society's understanding that a locker room is a private place" under the Fourth Amendment).[3]

Many state courts and legislatures, including the California Supreme Court, have recognized an expectation of privacy in location and phone records generally, and historical cell site information specifically. As more people live in states where these records are considered private, the government can no longer assert it is unreasonable to expect privacy in them. Thus, a probable cause search warrant is necessary to obtain historical cell site records.

A. Research Shows Americans Have a Subjective Expectation of Privacy in the Data Generated by Their Cell Phones.

For the Fourth Amendment to apply, a person must have an actual "expectation that his activities would be private." *Nerber*, 222 F.3d at 599 (citing *Bond v. United States*, 529 U.S. 334, 338 (2000). "Privacy does not require solitude," *United States v. Taketa*, 923 F.2d 665, 673 (9th Cir. 1991), and even when a person "cannot expect total privacy," he may nonetheless have an expectation of privacy from intrusions going beyond what he may otherwise anticipate. *Nerber*, 222 F.3d at 604.

Recent studies show Americans have an expectation of privacy in the data stored on and generated by their cell phones, including location information. In 2012, the Pew Research Center found that cell phone owners take a number of steps to protect access to their personal information and mobile data, and more than half of phone owners with mobile apps have uninstalled or decided

[3] The Ninth Circuit has even suggested that "a company's guarantee to its customers that it will safeguard the privacy of their records might suffice to justify resisting an administrative subpoena" in lieu of a warrant to obtain certain records. *United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108, 1116 (9th Cir. 2012).

to not install an app due to concerns about the privacy in their personal information. In addition, more than 30% of smart phone owners polled took affirmative steps to safeguard their privacy: 19% turned off location tracking on their phones and 32% cleared their browsing or search history.[4] The numbers are higher for teenagers, with Pew reporting 46% of teenagers turned location services off.[5] A 2013 survey conducted on behalf of the Internet company TRUSTe found 69% of American smart phone users did not like the idea of being tracked.[6] And a 2009 Carnegie Mellon survey of perceptions about location-sharing technologies showed that participants believed the risks of location-sharing technologies outweighed the benefits and were "extremely concerned" about controlling access to their location information.[7]

B. Courts Recognize the Privacy Implications of Location Information.

Gauging public apprehension about technologies shrinking privacy, an increasing number of courts across the country have recognized the privacy implications of location information. In 2012, the Supreme Court suggested in *United States v. Jones* that people expect their otherwise public movements on the street to remain private. 132 S. Ct. 945 (2012). Although the Court ultimately ruled placing a GPS tracking device on a car was a "search" because it was a physical trespass onto private property, in two separate concurring opinions, five members of the Supreme Court expressed concern that technology could intrude upon expectations of privacy. Critically, the concurring opinions of both Justice Sotomayor and Justice Alito (joined by four other justices) doubted that people reasonably expect their public movements would be monitored extensively. Justice Sotomayor questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain . . . their political

[4] Pew Research Internet Project, "Privacy and Data Management on Mobile Devices," (Sept. 5, 2012) http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.
[5] Pew Research Internet Project, "Location-Based Services" (Sept. 12, 2013) http://www.pewinternet.org/2013/09/12/location-based-services/.
[6] Truste, "TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size," (Sept. 5, 2013) http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size/.
[7] Janice Y. Tsai, *et al.* "Location-Sharing Technologies: Privacy Risks and Controls," Carnegie Mellon University, 12 (Feb. 2010) http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring). And Justice Alito wrote "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964 (Alito, J., concurring).

Last month, in *Riley v. California*, the Supreme Court specifically cited Justice Sotomayor's concurring opinion in *Jones* as a reason to limit police searches of cell phones incident to arrest. *Riley* recognized that cell phones store "qualitatively different" types of data compared to physical records, including data that can "reveal where a person has been," making it possible to "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Riley*, 134 S. Ct. at 2490 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)). *Riley* noted that because of data like this, the "scope of the privacy interests at stake" far exceeds that of anything in the physical world. *Id.* at 2491.

In the wake of *Jones*, several state and federal courts have also recognized the privacy implications of historical cell site data specifically. In protecting cell site data in *Commonwealth v. Augustine*, the Massachusetts Supreme Judicial Court recognized that this data may raise even greater privacy concerns than GPS tracking devices placed on a car because cell site data can track "the user's location far beyond the limitations of where a car can travel"—including into "constitutionally protected areas" like a home. 4 N.E. 3d 846, 861-62 (Mass. 2014). *Augustine* also noted historical cell site data gave police access to something it would never have with traditional law enforcement investigative methods: the ability "to track and reconstruct a person's past movements." *Id.* at 865. In *State v. Earls*, the New Jersey Supreme Court adopted a warrant requirement for historical cell site data, holding users should be "entitled to expect confidentiality in the ever-increasing level of detail that cell phones can reveal about their lives." 70 A.3d 630, 644 (N.J. 2013). Most recently, in *United States v. Davis*, the Eleventh Circuit noted that one may assume that location information that could be revealed by even one point of cell site data—such as a person's "first visit to a gynecologist, a psychiatrist, a bookie, or a priest"—is "private if it was not conducted in a public way." --- F.3d ---, 2014 WL 2599917, *8 (11th Cir. 2014).

While a person may take affirmative steps to broadcast her movements publicly—for example, by "checking in" or sharing her location over social media like Twitter or Facebook—historical cell site information is not "public" in this way. Instead, historical cell site information is private information disclosed to no one other than the phone company. *See Augustine*, 4 N.E.3d at 862-63. As explained below, just because technology is *capable* of disclosing what is otherwise private information about a person's specific location does not mean that a person has a lesser expectation of privacy under the Fourth Amendment.

II. THE "THIRD-PARTY DOCTRINE" DOES NOT CHANGE THE EXPECTATION OF PRIVACY IN HISTORICAL CELL SITE INFORMATION.

The government relies on *Smith v. Maryland* to argue cell phone users have no expectation of privacy in historical cell site records because that data has been exposed to a third party—the phone company. *See* Government's June 26, 2014 Letter Brief at p. 4 (citing *Smith*, 442 U.S. at 742-44). According to the government, when a person voluntarily uses a cell phone to make a call or respond to a text message, she knows the phone is sending information about her location to the cell phone company and thus cannot expect the phone company to keep that information private under *Smith*. But *Smith* does not alter the calculus here for two reasons.

First, cell phones present privacy issues vastly different from the technology at issue in *Smith*. The Supreme Court recently recognized this in *Riley*. In 1973, the Supreme Court in *United States v. Robinson* held police could search physical items—specifically a pack of cigarettes—found on an arrestee without a warrant incident to arrest. 414 U.S. 218, 236 (1973). But *Riley* refused to equate the cigarettes in *Robinson* with a modern cell phone, believing that comparing the two was "like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 134 S. Ct. at 2488. Instead, because modern cell phones implicate privacy concerns far beyond physical analogues addressed in past cases, any extension of reasoning from those past cases "to digital data has to rest on its own bottom." *Id.* at 2489.

Similarly, here, because the data generated by cell site information is so different in quantity and quality from the data generated by a simple landline phone, this Court cannot rely only on antiquated cases in determining how to protect data on and generated by cell phones. 134 S. Ct. at 2488-89. Instead, this Court should look to actual societal understandings of privacy in cell phone data and location information to determine the protections necessary to place on this information to satisfy the Fourth Amendment.

Second, *Smith* not only fails to capture the technology at issue here, it has also been rejected by the California Supreme Court. Just months after *Smith* was decided, the state high court ruled in *People v. Blair* that Californians have an expectation of privacy in their phone records under Article I, Section 13 of the state constitution, the state equivalent to the Fourth Amendment. 25 Cal. 3d 640, 655 (Cal. 1979).[8] While *Smith* held phone customers have no subjective expectation of privacy in dialed phone numbers because they "convey" the numbers to the company to have the calls connected, 442 U.S. at 742, *Blair* instead focused on the fact that a list of telephone calls provides a "virtual current biography" of a person. 25 Cal. 3d at 653. Since it was "virtually impossible for an individual" to "function in the modern economy without a telephone," these records were not voluntarily disclosed. *Id.* Thus, police need a warrant to obtain the records under the state constitution. *Id.* at 655; *see also People v. Chapman*, 36 Cal. 3d 98, 106-111 (1984), disapproved on other grounds in *People v. Palmer*, 24 Cal. 4th 856 (2001) (expectation of privacy in unlisted telephone number); *People v. McKunes*, 51 Cal. App. 3d 487, 492 (1975) (expectation of privacy in telephone company's customer records).[9]

---

[8] Article 1, section 13 of the California constitution states in whole "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated; and a warrant may not issue except on probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons and things to be seized."

[9] The California Attorney General has issued two opinions making clear that state law enforcement personnel must obtain a search warrant to install and use a pen register. First, in 1986, the Attorney General clarified that although California has no statutes governing pen registers, state magistrates were authorized to issue a search warrant supported by probable cause to permit police to install and use them. *See* 69 Ops. Cal. Atty. Gen 55 (1986). Later that year, Congress passed a set of federal statutes governing the installation and use of pen registers. *See* 18 U.S.C. §§ 3122-3127. Congress required state and federal law enforcement to obtain judicial authorization to install and

For this reason, the government's argument that cell phone users within this Court's jurisdiction in Northern California cannot expect location information to remain private once the data has been exposed to the phone company is incorrect. On the contrary, all Californians have been promised that third-party records generated by mundane but necessary acts, which reveal detailed biographical information about a person, are considered private.[10] That is precisely what historical cell site data is. Like bank records and dialed phone numbers, historical cell site information is capable of providing a "virtual current biography" of where a person has been, with whom they associate and their habits and patterns of movements. And, like these records, disclosing cell site records to a cell phone provider is not a truly voluntary act because it is virtually impossible to participate in contemporary society without generating them. *See Burrows*, 13 Cal. 3d at 247 (bank records protected by state constitution even though they are shared with a third party because it is "impossible to participate in the economic life of contemporary society without maintaining a bank account.").

Ultimately, that means this Court must reexamine the entire premise that *Smith* could be broad enough to encompass historical cell site records. At a minimum, the government cannot claim Californians have no subjective expectation of privacy in information the state has already promised its citizens is private, as finding no subjective expectation of privacy in these phone records would render state constitutional protection and *Blair's* rejection of *Smith* meaningless.

---

use a pen register but only required the government to demonstrate the evidence obtained via pen register is "relevant to an ongoing criminal investigation" rather than require probable cause. 18 U.S.C. §§ 3122(a)(2), (b)(2). For state law enforcement, the use of the federal pen register statute has to be consistent with state law. 18 U.S.C. § 3122(a)(2). So in 2003, the state Attorney General clarified that since *Blair* placed the information obtained from a pen register—a list of phone numbers dialed—within the "zone of privacy protected by the state Constitution," state law enforcement could not rely on federal law to install a pen register. 86 Ops. Cal. Atty. Gen. 198 at *3-4 (2003).

[10] The California Supreme Court has rejected the third-party doctrine in other contexts as well. For example, in *Burrows v. Super. Ct.*, the court held that California bank customers have an expectation of privacy in their bank records under the state constitution. 13 Cal. 3d 238, 247 (1974). Since a bank customer "reveals many aspects of his personal affairs, opinions, habits and associations" when dealing with a bank, the records are protected. *Id.* That conclusion is at odds with the U.S. Supreme Court's decision in *United States v. Miller*, 425 U.S. 435 (1976), which found no expectation of privacy in bank records.

III. THE NATIONWIDE TREND TOWARD GREATER PROTECTION FOR PRIVACY IN PHONE RECORDS AND LOCATION INFORMATION SHOWS SOCIETY RECOGNIZES A PRIVACY INTEREST IN THIS DATA IS REASONABLE.

Having established that advances in technology require changes in legal analyses, that people generally have a subjective expectation of privacy in their location, and that Californians specifically have an expectation of privacy in phone records and data capable of revealing a "virtual current biography" about a person, the question remains whether broader society is prepared to recognize that subjective expectation of privacy as reasonable. The answer is yes.

Immediately after *Smith* was decided, courts in eight states—including Colorado, Florida, Hawaii, Idaho, Illinois, New Jersey, Pennsylvania and Washington—followed California's lead and rejected *Smith*, instead finding those states' residents had a reasonable expectation of privacy under the state constitution in dialed phone numbers—notwithstanding the fact those records are held by the phone provider.[11] By statute, Georgia and Oregon required police to demonstrate probable cause to install and operate a pen register to obtain dialed phone numbers.[12]

Then, as technology continued to advance but before *Jones* was decided, the state supreme courts of New York, Oregon, and Washington held that people could reasonably expect privacy in their location, meaning that using technology to track a person's movements was a Fourth Amendment "search."[13] Five state legislatures passed statutes requiring police to obtain a probable cause search warrant to track a person's location with a tracking device like a GPS—even when the person is traveling in public places.[14] This meant that even before the Supreme Court addressed the

---

[11] *See People v. Sporleder*, 666 P.2d 135, 141-43 (Colo. 1983); *Shaktman v. State*, 553 So.2d 148, 150-51 (Fla. 1989); *State v. Rothman*, 779 P.2d 1, 7-8 (Haw. 1989); *State v. Thompson*, 760 P.2d 1162, 1165-67 (Id. 1988); *People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill.Ct.App. 1993); *State v. Hunt*, 450 A.2d 952, 955-57 (N.J. 1982); *Commonwealth v. Melilli*, 555 A.2d 1254, 1256-59 (Pa. 1989); *State v. Gunwall*, 720 P.2d 808, 813-17 (Wash. 1986); *see generally* Stephen E. Henderson, *Learning From all Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

[12] *See Ellis v. State*, 353 S.E.2d 19, 21-22 (Ga. 1987) (pen register is "device" under Ga. Code Ann. § 16-11-64(b) whose installation requires probable cause search warrant); O.R.S. § 165.663.

[13] *See, e.g., People v. Weaver*, 909 N.E.2d 1195, 1201 (N.Y. 2009) (GPS); *State v. Campbell*, 759 P.2d 1040, 1048-49 (Or. 1988) (use of radio transmitter to locate automobile); *State v. Jackson*, 76 P.3d 217, 223-24 (Wash. 2003) (GPS).

[14] *See* Haw. Rev. Stat. § 803-44.7(b); Okla. Stat. Ann. tit. 13, § 177.6(A); Or. Rev. Stat. Ann. §

question of whether Americans have a reasonable expectation of privacy in their location information, seven states, representing nearly 20% of the United States population[15] already recognized this privacy right.

After *Jones*, the number of people across the country reasonably expecting privacy in their location has increased, as more courts have recognized that an expectation of privacy in a person's location means technologies like GPS or real time cell phone tracking is a Fourth Amendment "search" under *Katz*.[16] *Jones* encouraged states to go further than they had before, particularly because Justice Sotomayor specifically questioned *Smith*, noting its "premise" was "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). Honing in on subjective expectations of privacy, she doubted "people would accept without complaint the warrantless disclosure" of information to the government like URLs they visit or the phone numbers they dial or text. *Id.*

As explained above, that has extended to historical cell site data, with the high courts of Massachusetts and New Jersey—relying in part on Justice Sotomayor's concurrence—recognizing a reasonable expectation of privacy in historical cell site data under their respective state constitutions and requiring police to use a search warrant to obtain that information. Five more states legislated privacy protections for historical cell site data, with Colorado, Maine, Minnesota, Montana and Utah passing statutes expressly requiring law enforcement to apply for a search warrant to obtain this data.[17] And more courts reached the same conclusions as Justice Sotomayor

---

133.619(6); 18 Pa. Cons. Stat. Ann. § 5761(c)(4); S.C. Code Ann. § 17-30-140(b)(2).

[15] This figure is based on 2013 population data for each state, as projected by the U.S. Census. *See* United States Census Bureau, "Quick Facts," http://quickfacts.census.gov/qfd/index.html.

[16] *Commonwealth v. Rousseau*, 990 N.E.2d 543, 552-53 (Mass. 2013) (GPS); *Commonwealth v. Rushing*, 71 A.3d 939, 961-64 (Pa. Sup. Ct. 2013), *appeal granted on other grounds* 84 A.3d 699 (2014) (cell phone signal); *State v. Brereton*, 826 N.W.2d 369, 379 (Wis. 2013) (GPS); *United States v. Powell*, 943 F. Supp. 2d 759, 776-77 (E.D. Mich. 2013) (real time cell site tracking); *State v. Zahn*, 812 N.W.2d 490, 496-499 (S.D. 2012) (GPS); *United States v. Lopez*, 895 F. Supp. 2d 592, 602 (D. Del. 2012) (GPS).

[17] *See* Colo. Rev. Stat. Ann. § 16-3-303.5(2); 16 Maine Rev. Stat. Ann. § 648; Minn. Stat. Ann. §§ 626A.28(3)(d), 626A.42(2) (effective August 1, 2014); Mont. Code Ann. § 46-5-110(1)(A); Utah Code Ann. § 77-23c-102(1)(a). A number of states have passed laws requiring police obtain a

in *Jones,* noting "the rapid expansion in the quantity of third-party data generated through new technologies raises important questions about the continued viability of the third-party doctrine in the digital age." *Augustine*, 4 N.E.3d at 863 n. 35; *see also State v. Walton*, 324 P.3d 876, 905 (Haw. 2014) (expectation of privacy in GNC membership account information).

Last month, the Eleventh Circuit Court of Appeals became the first federal appeals court to find an expectation of privacy in historical cell site records, holding police need a probable cause warrant to obtain them. *See Davis*, 2014 WL 2599917, *10.[18] Because *Davis* controls the actions of both federal and state law enforcement, people in Alabama, Florida and Georgia now have a reasonable expectation of privacy in historical cell site information. In sum, the number of people in the United States who have been promised by court decision or legislation that information about where they have been—either at a specific moment or over an extended period of time—has never been higher. While not dispositive of whether there is a Fourth Amendment expectation of privacy in historical cell site data, the growing number of people protected by the warrant requirement is compelling proof of "societal understandings" as to what level of privacy and security is reasonable.

Although the Eleventh Circuit's decision in *Davis* parts ways with the Fifth Circuit's decision in *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013), which found no expectation of privacy in historical cell site data, this Court writes on a blank slate. The Ninth Circuit has already suggested that *Smith* does not necessarily control all situations involving technology that captures information controlled by third parties. In *United States v. Forrester* the Court relied on *Smith* to find that the use of a pen register to capture IP address and other Internet metadata was not a Fourth Amendment "search." 512 F.3d 500, 509-11 (9th Cir.

---

search warrant only to track a cell phone in real time. *See, e.g.,* Ind. Code 35-33-5-12; Wisc. Stat. Ann. § 968.373(2).

[18] The Third Circuit Court of Appeals ruled in 2010 that a magistrate may, but is not required, to request the government apply for a search warrant to obtain historical cell site records. *In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records*, 620 F.3d 304, 319 (3d Cir. 2010).

2007). However, the court made clear it was not implying "more intrusive techniques or techniques that reveal more content-rich information" would lead to the same result. *Id.* at 511.

The opinions in *Davis*, *Augustine* and *Earls* and the state statutes requiring police obtain a warrant to get historical cell site records make clear that this location information is the more revealing and intrusive technique hinted at by *Forrester*. Coupled with the rejection of *Smith* in California law and the growing number of people for whom historical cell site data is protected by a warrant requirement, this shows the government must use a search warrant to obtain historical cell site data.

CONCLUSION

For more than 90% of Americans, a cell phone is the only phone they have. As anyone who moves about in society recognizes, cell phones are constantly in use in both public and private spaces. At the same time, they are also "constantly connecting to cell sites, and those connections are recorded" by cell phone companies. *Augustine*, 4 N.E.3d at 860. This means that Americans are constantly generating an almost unfathomable wealth of information about their whereabouts at all times.

When it comes to historical cell site records, it is clear that Americans generally and Californians specifically expect that the location information revealed by these records remain private. Given the growing trend in legislatures and courts across the country to protect this privacy interest by requiring a warrant, society understands this expectation of privacy is reasonable.

This court should follow the Supreme Court's lead in *Riley v. California* and recognize that, given the vast amount of data generated by cell phones, coupled with the trend toward greater privacy protections for that data, outdated cases cannot govern the outcome here. Americans have a reasonable expectation of privacy in the location data generated by cell site location information, and, as the Court noted in *Riley*, the answer to the question of what police must do before they may obtain that data "is simple—get a warrant." 134 S. Ct. at 2495.

DATED: July 29, 2014

Respectfully submitted,

By: _____

Jennifer Lynch
Hanni M. Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for *Amicus Curiae*
ELECTRONIC FRONTIER FOUNDATION

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on July 29, 2014, I filed the foregoing with the Clerk of the Court and caused to be served by U.S. Mail, postage thereon fully prepaid, a true and correct copy of the foregoing on:

Ellen Valentik Leonida
Federal Public Defender's Office
555 12th Street , Suite 650
Oakland, CA 94607-3627
(510) 637-3500
Fax: (510) 637-3507
Email: ellen_leonida@fd.org

Counsel for Defendant

Damali A. Taylor
U.S. Attorney's Office
450 Golden Gate Avenue, Box 36055
San Francisco, CA 94102
415-436-6401
Email: damali.taylor@usdoj.gov

Counsel for Plaintiff

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Dated this 29th day of July, 2014.

Stephanie Shattuck